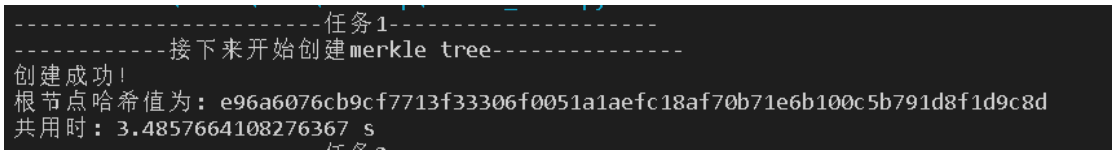
# Merkle tree 说明文档

## 任务 1：Construct a Merkle tree with 10w leaf nodes

代码说明：利用一个堆栈，不断地弹出前两个哈希值进行哈希，将新得到的哈希值再压入栈中，并对此创建新的节点存储。需要注意分辨叶子节点和非叶子节点，根据 RFC6962，叶子节点是在值前面加 0x00 进行哈希，非叶子节点是将两个孩子节点哈希合起来，并在前面加 0x01 再进行哈希，其余具体细节见注释以及详细代码

运行指导：直接运行 py 文件

运行截图：



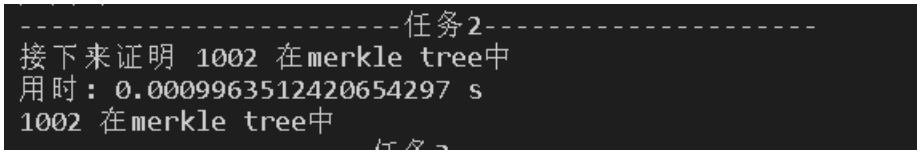

## 任务 2：Build inclusion proof for specified element

代码说明：merkle tree 的存在证明只需利用少量数据即可完成，对于某个区块 a，只需请求其兄弟区块 b 的哈希值可以算出它们两个的父节点为 hash(0x01+a+b)，接下来请求该父节点的兄弟节点的哈希值，

算出它们的父节点哈希值，利用同样的方法不断往上算，直到算到 merkle tree 的根节点，将这个值和 merkle tree 实际根节点的值相比较，若相等，即可证明该区块存在

运行指导：直接运行 py 文件

运行截图：




## 任务 3：Build exclusion proof for specified element

代码说明：要证明一个区块不在 merkle tree 中，通过先寻找 merkle tree 中比这个区块小的最大元素和比这个区块大的最小元素，然后通过证明二者是相邻节点，即可证明该区块不在 merkle tree 中

运行指导：直接运行 py 文件

运行截图：